# Protecting Consumer Information

Marti Phillips
Staff Attorney, SCDCA

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

***This presentation is not meant to serve as a substitute for reading the various laws discussed, seeking legal counsel or otherwise requesting Department guidance and/or interpretations on the laws it administers and enforces. The presentation merely serves as an introduction subject.***

# Roadmap

- SCDCA Overview
- ID Theft Background
- FIFITPA
- Federal Requirements
- Compliance Tips

# Department Overview

- Consumer Services & Education
- Public Information
- Consumer Advocate
- Administration
- Legal Division

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

UP NEXT: ID Theft Background

# What is Identity Theft?

- Unlawful use of your personal information
- Every 15 minutes, 200 people become victims of Identity Theft

  - **FTC= $50 billion losses annually**

  - **SC Stats: Consumer Sentinel**
    - **2011 – 20th**
    - **2010- 29th; 2009- 28th**
    - **2008- 29th; 2007- 30th**
    - **2006- 32nd ; 2005- 36th**

# How Does ID Theft Happen?

- You
- Friends and Family
- Lost or Stolen Wallets or Receipts
- Pre-approval Offers
- Dishonest Employees
  - **Skimming**
  - **Banks/ drs. office**
- Hoaxes
  - **Pretending to be Bank of America, etc & need personal info**
  - **Wachovia-Wells Fargo – “verify accounts”**
- Internet
  - **Phishing for pers’l information**

# CONSUMER SENTINEL NETWORK DATA BOOK

for January – December 2011

# Consumer Sentinel Network State Complaint Rates

*January 1 – December 31, 2011*

## Fraud & Other Complaints

| Rank | Consumer State | Complaints Per 100,000 Population[1] | Complaints |
|---|---|---|---|
| 1 | Colorado | 573.7 | 28,854 |
| 2 | Delaware | 552.2 | 4,958 |
| 3 | Maryland | 547.0 | 31,581 |
| 4 | Nevada | 530.3 | 14,320 |
| 5 | Virginia | 527.0 | 42,165 |
| 6 | Florida | 515.1 | 96,854 |
| 7 | Arizona | 503.7 | 32,195 |
| 8 | Washington | 473.4 | 31,832 |
| 9 | Ohio | 472.4 | 54,493 |
| 10 | New Jersey | 452.0 | 39,737 |
| 11 | New Hampshire | 451.8 | 5,948 |
| 12 | Missouri | 448.5 | 26,863 |
| 13 | Georgia | 447.9 | 43,395 |
| 14 | Alaska | 440.7 | 3,130 |
| 15 | Idaho | 433.2 | 6,790 |
| 16 | South Carolina | 426.3 | 19,720 |
| 17 | Pennsylvania | 425.3 | 54,027 |
| 18 | Tennessee | 425.3 | 26,987 |
| 19 | Oregon | 423.1 | 16,208 |
| 20 | California | 418.7 | 155,986 |
| 21 | Hawaii | 418.7 | 5,695 |
| 22 | Illinois | 407.4 | 52,278 |
| 23 | Montana | 406.3 | 4,020 |
| 24 | Texas | 406.1 | 102,107 |
| 25 | Connecticut | 404.2 | 14,447 |
| 26 | Alabama | 403.9 | 19,304 |
| 27 | Wyoming | 403.8 | 2,276 |
| 28 | Massachusetts | 400.8 | 26,245 |
| 29 | Wisconsin | 399.8 | 22,736 |
| 30 | North Carolina | 399.2 | 38,063 |
| 31 | Louisiana | 397.1 | 18,000 |
| 32 | Utah | 394.2 | 10,895 |
| 33 | Kansas | 393.4 | 11,225 |
| 34 | Indiana | 390.1 | 25,296 |
| 35 | New Mexico | 389.6 | 8,023 |
| 36 | New York | 387.9 | 75,163 |
| 37 | Rhode Island | 380.4 | 4,004 |
| 38 | Michigan | 374.4 | 37,007 |
| 39 | Nebraska | 373.6 | 6,824 |

## Identity Theft Complaints

| Rank | Victim State | Complaints Per 100,000 Population[1] | Complaints |
|---|---|---|---|
| 1 | Florida | 178.7 | 33,595 |
| 2 | Georgia | 120.0 | 11,625 |
| 3 | California | 103.6 | 38,607 |
| 4 | Arizona | 98.5 | 6,296 |
| 5 | Texas | 96.1 | 24,162 |
| 6 | New York | 92.3 | 17,880 |
| 7 | Nevada | 89.9 | 2,427 |
| 8 | New Jersey | 86.4 | 7,599 |
| 9 | Maryland | 86.3 | 4,980 |
| 10 | Delaware | 83.5 | 750 |
| 11 | Colorado | 82.6 | 4,156 |
| 12 | Alabama | 82.5 | 3,942 |
| 13 | Michigan | 82.1 | 8,119 |
| 14 | Illinois | 80.8 | 10,361 |
| 15 | Pennsylvania | 79.2 | 10,061 |
| 16 | New Mexico | 78.2 | 1,610 |
| 17 | Mississippi | 74.5 | 2,210 |
| 18 | Washington | 72.2 | 4,853 |
| 19 | Missouri | 71.5 | 4,282 |
| 20 | South Carolina | 68.5 | 3,168 |
| 21 | Virginia | 67.7 | 5,416 |
| 22 | Connecticut | 67.5 | 2,413 |
| 23 | Tennessee | 67.4 | 4,275 |
| 24 | Kansas | 67.1 | 1,914 |
| 25 | North Carolina | 65.9 | 6,287 |
| 26 | Ohio | 64.8 | 7,479 |
| 27 | Louisiana | 64.7 | 2,934 |
| 28 | Arkansas | 63.9 | 1,862 |
| 29 | Massachusetts | 63.0 | 4,128 |
| 30 | Rhode Island | 58.3 | 614 |
| 31 | Oregon | 58.1 | 2,226 |
| 32 | Oklahoma | 56.4 | 2,115 |
| 33 | Indiana | 54.8 | 3,555 |
| 34 | Utah | 54.8 | 1,514 |
| 35 | Minnesota | 50.4 | 2,671 |
| 36 | Wyoming | 49.7 | 280 |
| 37 | Wisconsin | 48.9 | 2,782 |
| 38 | Nebraska | 47.6 | 869 |
| 39 | New Hampshire | 46.9 | 617 |

# Identity Theft Complaints Count from South Carolina Victims = 3,168

## *Identity Theft Types Reported by South Carolina Victims*

| Rank | Identity Theft Type | Complaints | Percentage[1] |
|---|---|---|---|
| 1 | Government Documents or Benefits Fraud | 764 | 24% |
| 2 | Phone or Utilities Fraud | 461 | 15% |
| 3 | Credit Card Fraud | 334 | 11% |
| 4 | Bank Fraud | 248 | 8% |
| 5 | Employment-Related Fraud | 205 | 6% |
| 6 | Loan Fraud | 130 | 4% |
| | Other | 829 | 26% |
| | Attempted Identity Theft | 204 | 6% |

[1]Percentages are based on the 3,168 victims reporting from South Carolina. Note that CSN identity theft complaints may be coded under multiple theft types.

# Financial Identity Fraud and Identity Theft Protection Act (FIFITPA)

- Legislative Background
- Consumer Id Theft Protection
- Social Security Numbers
- Records Disposal
- Security Breach
- Other Protections

# Legislative Background

- Bills
- Comprehensive Result= S. 453, Act 190
- Current Status
  - *Effective dates ~ December 31, 2008 & July 1, 2009*

# Consumer ID Theft Protection

Sections 37-20-110 et seq.

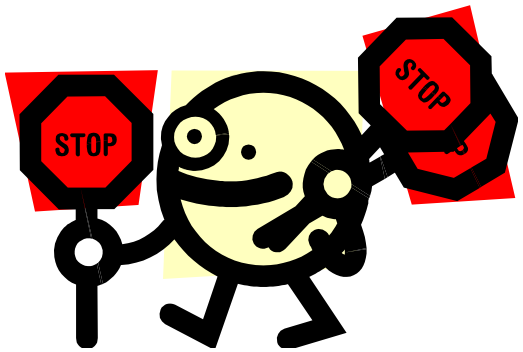
- Security Freeze
- Right to Dispute
- Social Security Numbers
- Records Disposal
- Security Breaches

# Consumer ID Theft Protection cont…

- Security Freeze~
- ***In General***
  - **Freeze**- credit report cannot be accessed without consumer's permission
  - Available to **ANYONE**
  - Submit request to CRA
    - Certified letter or e-mail
  - CRA must place within 5 days

# Consumer ID Theft Protection cont…

- Security Freeze cont…
  - **To Thaw** (temporarily remove freeze)
    - Request via e-mail, fax, telephone, etc.
    - Can be for a specified time or creditor/ requestor
    - CRA must thaw within 15 minutes
  - **To Lift**
    - Request via e-mail, telephone, etc
    - CRA must remove within 3 days



# Consumer ID Theft Protection cont…

- Security Freeze cont…
  - It is ***FREE*** to:
    - Place,
    - Temporarily Lift OR
    - Remove

A Security Freeze!!!

# Consumer ID Theft Protection cont…

- Right to Dispute- ***FIFITPA Mirrors FCRA Dispute Provisions***
  - Fair Credit Reporting Act
    - ***Consumer Can Dispute***:
      - Inaccurate, incomplete or untimely items
      - To credit reporting agency "CRA" and/or
      - Furnisher (Creditor)
    - ***Requirements***:
      - CRA - Notify furnisher within 5 days
      - CRA & Furnisher - Investigate (unless frivolous)
      - CRA & Furnisher - Note File= in dispute
      - If no resolution in 30 days, CRA must remove info
    - ***Resolution***
      - Notify consumer within 5 days
      - 100 word dispute

# Consumer ID Theft Protection cont…

- Reporting Periods - FCRA
  - *Bankruptcy*
    - 10 years
  - *Civil Lawsuit or Judgment*
    - 7 years or statute of limitations (longer)
  - *Paid Tax Lien*
    - 7 years
  - *Accounts Placed in Collection OR Charged Off*
    - 7 years (clock begins 180 days after delinquency)
  - *Other Adverse Info*
    - 7 years

# Consumer ID Theft Protection cont…

- Right to Dispute~ FIFITPA Additions
  - **If CRA DENIES inaccuracy MUST:**
    - Give basis;
    - Send copy of file, including which creditors were contacts;
    - Give evidence that info is accurate
  - **If CRA ADMITS inaccuracy MUST**:
    - Contact creditors/requestors from the last six months

# Consumer ID Theft Protection cont…

- Right to Dispute cont…
  - Private Cause of Action
  - Department of Consumer Affairs to Enforce
    - Complaints
      - 1-800-922-1594
      - www.scconsumer.gov "Complaint Services"
    - Pattern or Practice

UP NEXT: Social Security Numbers

# Social Security Numbers

## Section 37-2-180/ 30-2-310

- Among other prohibitions, a public body or a business may not:
  - Make available to the public a person's social security number or six or more digits of the number;
  - Intentionally print or imbed a person's social security number or six or more digits of the number on a card required for access to a product or service;
  - **Require a person to transmit a social security number or six or more digits of the number over the internet UNLESS there is a (1) secure connection or (2) the number in encrypted.**

# Social Security Numbers cont…

- **Require a person to use his/her social security number or six or more digits of the *number to access the web* unless a password is also required;**

- Print a person's social security number or six or more digits of the number **on materials mailed** to that person UNLESS ***state or federal law requires*** it;

- ***May not collect a person's social security number* or six or more digits of the number UNLESS the body is (1) authorized by law or (2) the collection is imperative to the body performing its duties and responsibilities;**

# Social Security Numbers cont…

- When collecting a person's social security number or six or more digits of the number, must separate the number from the rest of the record, ***or as otherwise appropriate, so the number can be easily redacted pursuant to a FOIA request***;

- At a person's request, ***must give a statement of purpose*** for collecting the person's social security number or six or more digits of the number and how it will be used.

# Social Security Numbers cont…

- Exceptions:
  - SS # is included in an application. (*Still cannot be on a postcard or visible on or thru an envelope.)*
  - Opening of an account or payment for a product or service authorized by the consumer.
  - Person providing the SS# to a governmental authority.

UP NEXT: Records Disposal

# Records Disposal

- Definitions~ **Effective 12-31-2008**
  - ***Personal Identifying Information (PII)***
    - Consumer's 1st name or 1st initial
    - + last name
    - +unencrypted or unredacted:
      - Social security #, or
      - Driver's License #, or
      - Financial account #, credit card, debit card + security code, or
      - Other #s or information to get access to financial accounts

# Records Disposal cont…

- Definitions cont…
  - ***Business***
    - Person conducting business in this State
  - ***Disposal***
    - discarding records that contain *personal identifying information* OR
    - the sale, etc of anything containing

# Records Disposal cont…

- Disposal of Records~
  - Hardware & Storage Media
    - B4 transfer or disposal must:
      1. *Remove pers'l & confdt'l information*
  - Record
    - If PII involved, B4 disposal:
      1. *Shred, erase the PII to make unreadable or undecipherable*

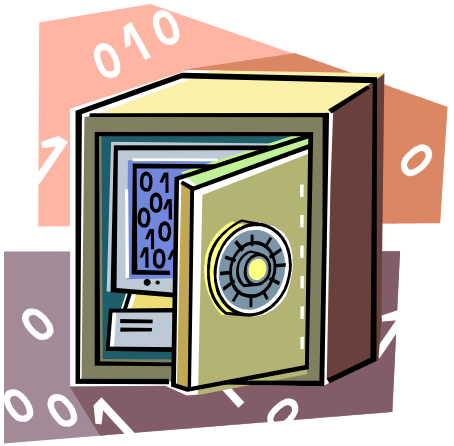
***Can hire a 3rd party to dispose of records= ok if compliant***

# Records Disposal cont…

- Penalties
  - Civil Action
    - Department
    - Consumer
      - 3x actual damages/ limit $1,000 + attorneys fees
      - Injunction
  - Administrative Action
    - Injunctions
    - Fines

UP NEXT: Security Breaches

# Security Breach~ **Effective 7-1-2009**




- **Definitions~**
  - ***Security Breach***
    - *Unauthorized access to AND*
    - *Acquisition of:*
      - *Records/ data containing PII*
      - *Illegal use has or is likely to occur*
  - ***Breach of the Security of the System***
    - *Unauthorized access to AND*
    - *Acquisition of:*
      - *Computerized data (where PII isn't encrypted, redacted, etc)*
      - *Illegal use has or is likely to occur*

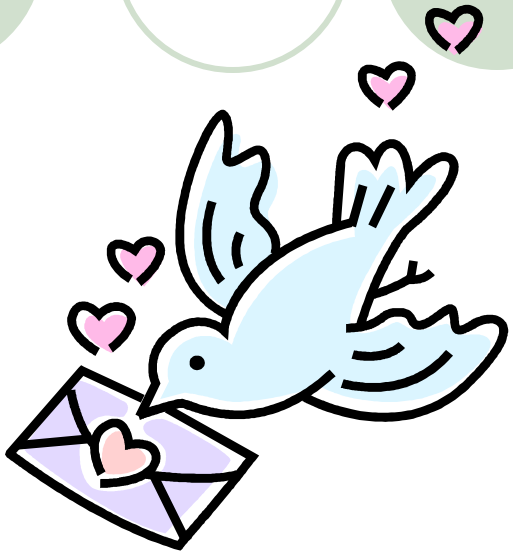
# Security Breach cont…

- **Applies to:**
  - Persons conducting business in this State

- **Notification~Section 1-11-490**
  - **To Consumer When**:
    - Computerized or other data
    - containing PII that was not encrypted or redacted
    - Was, or is reasonably believed, to have been acquired by an unauthorized person
    - When illegal use of the PII occurred, is likely to occur or material risk to person

# Security Breach cont…

- **Notification cont…~**
  - **Must be Made:**
    - **Without delay**
    - **BY:**
      - **Written notice**
      - **Electronic notice (if primary method)**
      - **Telephone notice;**
      - **Substitute Notice: $250k or 500,000 persons**
        - **E-mail notice;**
        - **Webpage notice;**
        - **Notify statewide media**



# Security Breach cont…

**Sample Security Breach Notification Letter**

Date

Organization's Name and Address
Affected Person's Name and Address

**Dear (Person's Name):**

**I am writing to inform you that our organization experienced** *(or discovered)* **a security breach on or about** *(date of breach or when breach was discovered).* **Unfortunately this has resulted in unauthorized access to your personal identifying information, specifically your** *(identify information that was or is reasonably believed to have been acquired).* *(Organization Name)* **is taking this matter very seriously and has** (*describe steps taken to prevent further harm or access to the person's personal identifying information and indicate whether or not law enforcement and/ or the Department of Consumer Affairs was notified of the breach).* **If you have any questions about this notice, please contact** *(name of contact person)* at *(contact's telephone number).* **You may also contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for information on steps you can take to defend yourself against identity theft**.

**Sincerely,**

# Security Breach cont…

- **Notification cont…~**
  - **To the Department When:**
    - **> 1,000 persons affect @ 1 time**
    - **Must also notify national consumer reporting agencies**
  - **Notice Must Include:**
    - **Timing,**
    - **Distribution, and**
    - **Content of Notice**

**Mail To:**

**Legal Division**

**RE: Security Breach Notification**

**South Carolina Department of Consumer Affairs**

**P.O. Box 5757**

**Columbia, SC 29250**

# Security Breach cont…

- **Penalties:**
  - Private Cause of Action
    - Damages,
    - Injunction, and
    - Attorney's fees
  - Administrative Fines
    - Willful violation
    - Up to $1,000 per affected person

# SCDCA Security Breach Report

- Notification letters sent to SCDCA by companies and governmental entities reporting security breaches from

  July 2008 - July 2011. (Eff. 7/1/09)

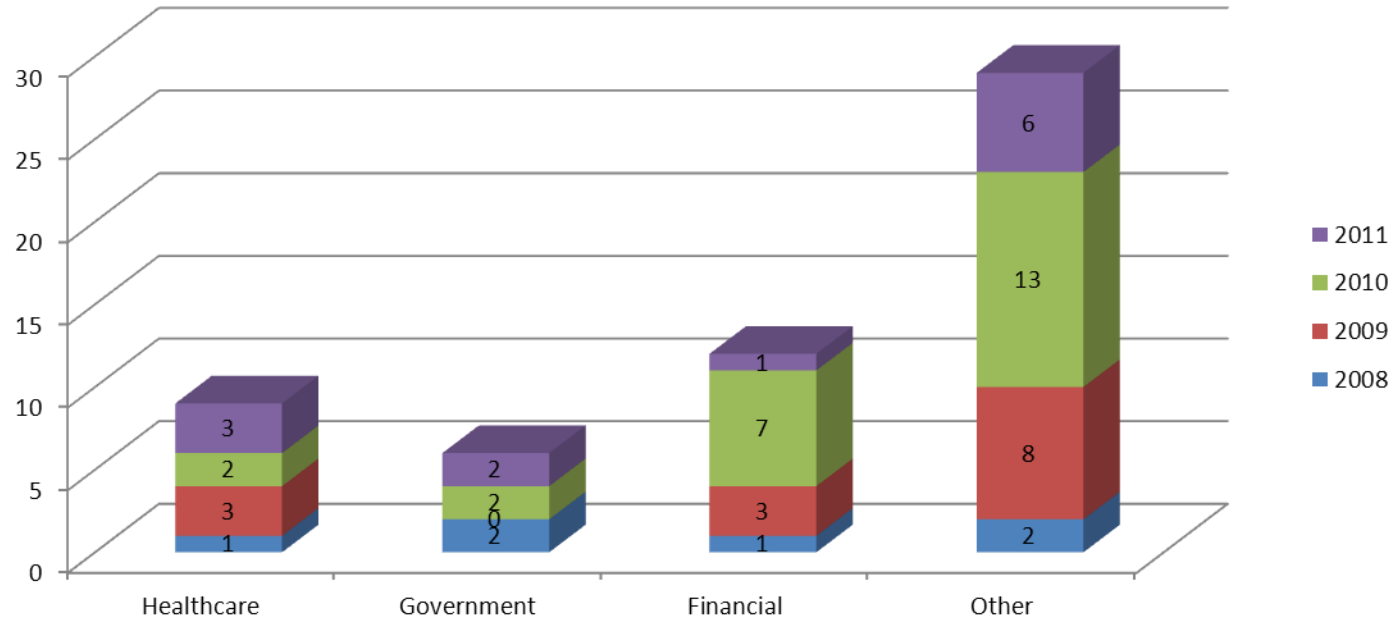
- Many companies did not report a specific number of consumers affected. Therefore, the totals provided reflect the minimum number of South Carolina residents potentially affected.

# Security Breach Report cont…

- During the designated time period, the Department received:
  - 56 security breach notices affecting 410, 865 South Carolina residents.

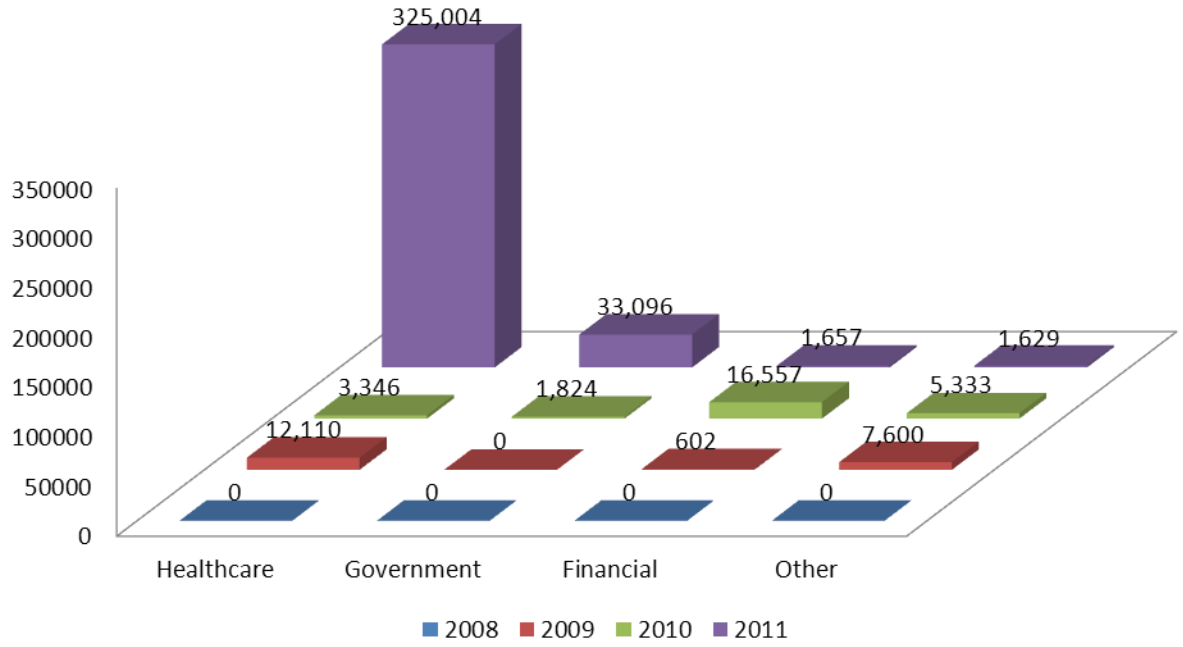
- Top Categories:
  - Healthcare organizations,
  - governmental entities, and
  - financial service providers

# Security Breach Report cont…



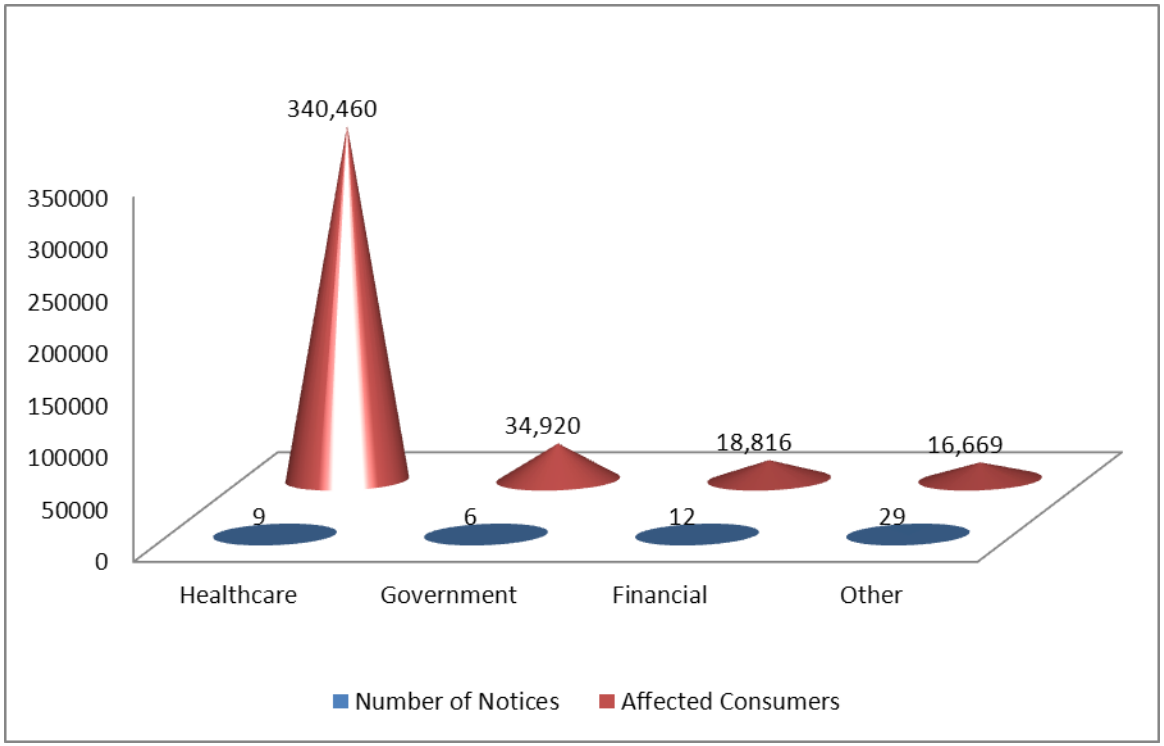

- 9- healthcare organizations
- 6 - governmental entities
- 12 - financial services providers
- 29- other reports

# Security Breach Report cont…




- July 1, 2009- Dec. 2009 ~ 20,312 affected residents
- 2010 ~ 27,060 affected residents
- 2011 ~  361,386 affected residents

# Security Breach Report cont…




- Healthcare industry- 9 security breach notices that affected more than 340,000 South Carolina residents.
- Government notices- 6 breaches with almost 35,000 consumers affected.
- Financial organizations- 12 breaches affecting almost 19,000 consumers
- “Other industries”- 29 notices affecting approximately 17,000 consumers.

SCDCA Home Page - Windows Internet Explorer

http://www.scconsumer.gov/

ent Book - no tabbed address section

No code AutoFill Code

AT-A-GLANCE... - Search | SCDCA Home Page

Page Tools

Google™ Custom Search Search

click here to File a Complaint
click here to Email Consumer Affairs

## Spot Light

Don't Be Deceived By Telephone Scams

***SCDCA TV***
(Click Image Below)


- Licensing, Registrations & Filings
- Buyer Beware
- About DCA
- Contact DCA
- FAQs
- Complaint Services
- Legal Division
- Press Room
- Publications
- Consumer Education
- Related Links
- Recalls
- Multimedia

## Recent Consumer News from SCDCA

Options Announced for Consumers Harmed During the Foreclosure Process

Commission on Consumer Affairs Names Lybarker SCDCA Administrator

Florence County High School Essay Contest Details
Essay Contest Letter
Essay Contest Guidelines
Statement of Assurance

South Carolina Credit Counseling Fall 2011 Webinar Schedule

LifeSmarts 2011-2012 is Underway

SCDCA to Participate in Florence Library Fall Festival

SCDCA to Participate in FREE Foreclosure Forum

SCDCA Issues Inaugural Security Breach Report

Security Breach Notice Report

ALERT: Former Members of ZX Fitness

Mortgage Disclosure Forms Getting a Makeover

Mortgage Fraud Hotline Data Supports Supreme Court Order

Debt Collection Complaints Top Listing; $580,000 Back to Consumers

**Spring 2011 Consumer Alert** - Test Your Financial Literacy IQ - April is Financial LiteracyMonth. SCDCA could not thinkof a better time to help you increase your financial literacy IQ.

2011"If I Had $100, I Would...." Essay Contest. Click here to view the

Internet 100%

start | 3 Microsoft Word | 2 Novell Group... | SCDCA Home P... | Conferences | Reports | 3 Microsoft Po... | Emergency Reg... | 11:39 AM

Complaint Services
Legal Division
Press Room
Publications
Consumer Education
Related Links
Recalls
Multimedia

***Federal Reserve System Credit Card Calculator***

***Identity Theft FIFITPA***

Mortgage Disclosure Forms Getting a Makeover

Mortgage Fraud Hotline Data Supports Supreme Court Order

Debt Collection Complaints Top Listing; $580,000 Back to Consumers

**Spring 2011 Consumer Alert** - Test Your Financial Literacy IQ - April is Financial LiteracyMonth. SCDCA could not thinkof a better time to help you increase your financial literacy IQ.

2011"If I Had $100, I Would...." Essay Contest. Click here to view the winning essays.

SCDCA Reaches Social Media Milestones (PDF)

SCDCA Recognized for Consumer Publication (PDF)

SCDCA Announces Launch of Mortgage Log System (PDF)

**What is this with the high gasoline prices?**

**2011 Palmetto Affordable Housing Forum.** The presentation materials for the seminars presented by SCDCA at the 2011 Palmetto Affordable Housing Forum can be found by clicking here. The slides may not be used for any purpose without the presenter's written consent.

**Commission on Consumer Affairs Names Carri Lybarker SCDCA Acting Administrator** (PDF)

Internet 100%

start | 3 Microsoft Word | 2 Novell Group... | SCDCA Home P... | Conferences | Reports | 3 Microsoft Po... | Emergency Reg... | 11:41 AM

SCDCA Home Page - Windows Internet Explorer

http://www.scconsumer.gov/identity_theft.html

ent Book - no tabbed address section

No code | AutoFill Code

AT-A-GLANCE... - Search | SCDCA Home Page

Page | Tools

Google™ Custom Search | Search

click here to File a Complaint
click here to Email Consumer Affairs

Consumer Affairs Hosts Webinars for Consumers and Businesses
Webinar Registration Forms click here

***SCDCA TV***
(Click Image Below)


Whats New!
Licensing, Registrations & Filings
Buyer Beware
About DCA

## IDENTITY THEFT INFORMATION

- **Presentations**
  - Identity Theft & Data Security (PDF)
  - South Carolina's New Privacy Law (PDF)
  - Responding to Data Security Breaches (PDF)
  - Incident Response Security Breaches (PDF)
- **Handouts**
  - SCDCA- Identity Theft & The Law (PDF)
  - FTC Safeguards Rule (PDF)
  - FTC Information Compromise (PDF)
- **For Consumers**
  - FIFITPA Brochure (PDF)
- **Other Important Information**
  - Financial Identity Fraud and Identity Theft Protection Act
  - OCC Guidelines (PDF)
  - FTC Disposal Rule (PDF)
  - DSIT Information Security Policy (PDF)
  - DSIT- Hardware Sanitization Policy (PDF)
  - DSIT Incident Management Policy (PDF)

UP NEXT: Federal Laws

# Federal Requirements

- Fair Credit Reporting Act (“FCRA”)
- Disposal Rule *(FCRA)*
- Financial Privacy Rule *(Gramm-Leach-Bliley Act (“GLB”))*
- Safeguards Rule *(GLB)*
- Red Flags Rule *(FCRA – FACTA)*

# Federal Requirements cont…

- History
  - Original Eff. Date= 1971
    - Amended at least 6 times since
  - Most recent major~
    - Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- Purpose
  - Promote accuracy & fairness in credit reporting arena
    - Places requirements on:
      - credit reporting agencies
      - Furnishers of information
    - Provides consumer protections

# Federal Requirements cont…

- FCRA – What is it?
  - Accuracy and fairness in credit reporting (more later)
  - Free annual credit reports
  - Identity Theft Protections
    - Fraud Alerts
    - Blocking of Information
    - Disposal Rule
    - Red Flags Rule

# Federal Requirements cont…

- Definitions: 15 U.S.C. 1681a
  - *Consumer report:*
    - Any communication of information by a credit reporting agency
    - Contains info on a consumer's
      - *Credit worthiness*
      - *Credit standing*
      - *Character*
      - *General reputation*
      - *etc*
    - Info is used or collected as a factor in deciding if a consumer is eligible for:
      - *Credit, insurance, employment, etc*

# Federal Requirements cont…

- **Disposal Rule (FCRA)**
  - **Requires proper disposal of sensitive information derived from consumer reports.**
    - **Who?**
      - **Any person who uses a consumer report for business purposes, ie: lenders, insurers, employers, landlords, mortgage brokers and debt collectors.**
    - **How?**
      - **Burn, pulverize, shred**
      - **Destroy or erase electronic data**
      - **Due diligence in selecting and monitoring contractors.**

# **Federal Requirements** cont…

- **Red Flag Rule (FACTA)**
  - **Requires financial institutions and creditors* to develop a *written program* that identifies and detects relevant warning signs ("Red Flags") of Identity Theft.**
  - **Program must include** policies and procedures that enable a financial institution or creditor to:
    - Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible id theft;
    - Detect red flags that have been incorporated into the Program;
    - Respond appropriately to any red flags; and
    - Ensure the Program is updated periodically to reflect changes in risks from id theft.

# **Federal Requirements** cont…

- **Red Flag Rule (FACTA)**
  - **Who?**
    - state or national bank, S & L, Credit Union that holds a deposit account or an account where the consumer makes transfers,
    - entity that regularly extends, renews, or continues credit. Includes finance companies, auto dealers, mortgage brokers, utility companies, and telecommunication companies.
  - **How?**
    - FTC, Banking Agencies, and NCUA have published Guidelines suggesting 26 possible red flags.

# Examples

- Alerts or warnings from a consumer reporting agency.
- Suspicious documents.
- Suspicious personal identifying information.
- Unusual use of or activity in a covered account.
- Notices from customers, IDT victims, law enforcement or other businesses.

# FCRA Cont…

- Penalties: 15 U.S.C 1681n&o
  - ***Civil Liability***
    - Willful,
    - Knowing or
    - Negligent noncompliance
  - ***Administrative Enforcement:*** 15 U.S.C 1681s
    - *Federal Trade Commission*
      - Primary enforcer
    - *State Action*
      - FTC 1st right to refuse

# **Federal Requirements** cont…

- **Gramm-Leach-Bliley Act**
  - **What is it?**
    - **opening up competition among banks, securities companies and insurance companies**
    - **Privacy Protections**
  - **Financial Privacy Rule (Gramm-Leach-Bliley Act)**
  - **Safeguards Rule (Gramm-Leach-Bliley Act)**
    - Apply to **financial institutions***

***CAUTION~ Definition very BROAD**

# **Federal Requirements** cont…

- **Financial Institutions: all businesses, regardless of size, that are "significantly engaged" in providing financial products or services.**
- **Examples include:**
  - **auto dealers,**
  - **mortgage brokers,**
  - **credit counselors,**
  - **realtors,**
  - **tax preparers, &**
  - **courier services.**

# **Federal Requirements** cont…

- **Financial Privacy Rule (Gramm-Leach-Bliley Act)**
  - protects a consumer's "nonpublic personal information" (NPI)
    - *NPI Is:*
      - *any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available."*

# **Federal Requirements** cont…

- **Financial Privacy Rule (Gramm-Leach-Bliley Act) cont…**
  - All customers must be given a privacy notice. You must provide an "initial notice" by the time the customer relationship is established.
    - Notice Must Include description of:
      - how you collect, disclose, and protect NPI about consumers and customers, including former customers.
  - If you share NPI with nonaffiliated third parties, you also must give your customers opportunity to opt-out (exemption do apply)

# **Federal Requirements** cont…

- **Safeguards Rule (Gramm-Leach-Bliley Act)**
- Requires **financial institutions*** to develop and implement safeguards to protect customer information.
- Companies must:
  - Develop a written information security plan
  - Designate employee(s) to coordinate safeguards
  - Identify and assess risks to customer information
  - Design and implement a safeguards program (regularly monitor, test, and update it)
  - Oversee service providers

# **Federal Requirements** cont…

- **Safeguards Rule (Gramm-Leach-Bliley Act) cont…**
  - **Financial Institutions: all businesses, regardless of size, that are "significantly engaged" in providing financial products or services.**
  - **Examples include auto dealers, mortgage brokers, realtors, tax preparers, & courier services.**

UP NEXT: Compliance Tips

# ID Theft Prevention Tips

- Written information security plans
- Other Tips


# Written Information Security Plans

*(Safeguards Rule Requirement= written information security plan)*

- There are three areas that are especially important when thinking about the risks to your business:

1. Employee Management & Training
2. Information Systems
3. Detecting and Managing System Failures

*Companies should implement plans appropriate for their business!*

# 1. Employee Management & Training

- Check references and run background checks on employees that will have access to customer information.
- Have employees sign an agreement to follow your company's confidentiality and security standards for handling customer information.
- Limit access to customer information to employees that have a business reason to see it.
- Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis (passwords of 6+ characters that use upper- and lower-case letters, combining letters, numbers and symbols).

# 1. Employee Management & Training, continued…

- Use password-activated screen savers to lock access to computers after a period of inactivity.
- Develop policies for appropriate use and protection of laptops, PDAs, cell phones and other mobile devices.
- Train employees to take basic steps to protect customer information, such as:
  - Lock rooms and file cabinets where records are kept
  - Not posting employee passwords in work areas
  - Encrypting sensitive customer information and it is transmitted electronically via public networks
  - Refer calls or requests for customer information to individuals that have been trained in the company's safeguard procedures
  - Reporting suspicious attempts to obtain customer information

# 1. Employee Management & Training, continued…

- Remind employees of your company's policy- and the legal requirement- to keep customer information secure and confidential
- Impose disciplinary measures for employees that violate these measures
- Immediately deactivate any usernames and passwords for terminated employees to prevent access to customer information

# 1. Employee Management & Training, continued…

- Know where customer information is stored and store it securely:
  - Make sure storage areas are protected from destruction or physical damage (such as fire or flood)
  - Store customer records in a room or cabinet that is locked when unattended
  - When customer information is stored on a computer or server, use a “strong” password and make sure that equipment is kept in a physically secure-area.
  - Where possible, avoid storing customer information on a server or computer with an internet connection
  - Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area
  - Maintain a careful inventory of where sensitive customer information may be stored.

# 2. Information Systems

- Take steps to ensure secure transmission of customer information
  - Use a Secure Sockets Layer (SSL) or other secure connection when transmitting credit card information
  - When collecting information online, make secure transmission automatic and caution customers about transmitting sensitive data via email in response to unsolicited messages
  - Encrypt data when transmitting sensitive data by email over the internet.

# 2. Information Systems continued…

- Dispose of customer information in a secure way:
  - Consider a records retention manager to supervise the disposal of records containing customer information. If hiring an outside firm, take steps to ensure they are reputable.
  - Burn, pulverize, or shred papers containing customer information so this data cannot be read or reconstructed.
  - Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

# 3. Detecting and Managing System Failures

Take reasonable steps to prevent attacks, quickly diagnose a security incident, and have a plan in place to respond effectively. Business should consider:

- Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.

- Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:
  - check with software vendors regularly to get and install patches that resolve software vulnerabilities;
  - use anti-virus and anti-spyware software that updates automatically;
  - maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations;
  - regularly ensure that ports not used for your business are closed; and
  - promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

# 3. Detecting and Managing cont…

- Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:
  - keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
  - use an up-to-date intrusion detection system to alert you of attacks;
  - monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
  - insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.

# 3. Detecting and Managing cont…

- Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:

  - take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;

  - preserve and review files or programs that may reveal how the breach occurred; and

  - if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible

# 3. Detecting and Managing cont…

- Notifying law enforcement,consumers and/or businesses in the event of a security breach:

- ***Notifying Law Enforcement***
  - When the compromise could result in harm to a person or business, call your local police department immediately.
  - If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service.
  - For incidents involving mail theft, contact the U.S. Postal Inspection Service.

# 3. Detecting and Managing cont…

- ***Notifying Consumers***
  - consult with your law enforcement contact about the timing of the notification so it does not impede the investigation.
  - designate a contact person within your organization for releasing information.
  - describes clearly what you know about the compromise. Include how it happened; what information was taken, and, if you know, how the thieves have used the information; and what actions you have taken already to remedy the situation. Explain how to reach the contact person in your organization. Consult with your law enforcement contact on exactly what information to include so your notice does not hamper the investigation.
  - explains what responses may be appropriate for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports. See www.ftc.gov/idtheft for more complete information on appropriate follow-up after a compromise.

# 3. Detecting and Managing cont…

- include current information about identity theft. The FTC's Web site at www.ftc.gov/idtheft has information to help individuals guard against and deal with identity theft.

- provides contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use. Be sure to alert the law enforcement officer working your case that you are sharing this contact information.

# 3. Detecting and Managing cont…

- ***Notifying Businesses***

- Information compromises can have an impact on businesses other than yours, such as banks or credit issuers.
  - If account access information — say, credit card or bank account numbers — has been stolen from you, but you do not maintain the accounts, notify the institution that does so that it can monitor the accounts for fraudulent activity.
  - If you collect or store personal information on behalf of other businesses, notify them of any information compromise, as well.

- If names and Social Security numbers have been stolen, you can contact the major credit bureaus for additional information or advice.
  - If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts for their files.
  - Your notice to the credit bureaus can facilitate customer assistance.
  - ***(required when more than 1,000 persons are affected by a breach ~ SC law)***

# Other Tips

- Copier Data Security
  - http://business.ftc.gov/documents/bus43-copier-data-security
- Reducing risks to your computer systems
  - http://business.ftc.gov/documents/bus58-security-check-reducing-risks-your-computer-systems
- Writing effective financial privacy notices
  - http://business.ftc.gov/documents/bus55-getting-noticed-writing-effective-financial-privacy-notices

Marti Phillips
803-734-4241

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

**Toll Free: 1-800-922-1594**

**Fax: 803-734-4229**

**www.scconsumer.gov**